University of Reading

IT INCIDENT CRITERIA

Guidance on priorities to be used when logging incidents

Contents

Version control

VERSION	KEEPER	REVIEWER	CHANGE	DATE
1.0	ITS	Gordon Roberts		
1.1	IT	Ian Bland	Updated and expanded	22/01/2016
1.2	IT	Ian Bland	Formatted and updated	04/09/2017

Introduction

This document is to provide guidelines for setting the initial priority of incidents and requests reported to IT and the expected response and resolution times. While prioritisation of incidents is a key part of the Incident Management process, the need to resolve service failures within an appropriate time is also a key component of Service Level Management. This document is therefore jointly owned by the Process Owners for both Incident Management (Luke Chapman) and Service Level Management (Ian Bland). Please direct queries to either or both of these people.

Definitions (ITIL)

Incident	An unplanned interruption to an IT service or reduction in the quality of an IT service. The failure of a Configuration Item (CI) that has not yet affected service is also an incident.
Service Request	A formal request from a user for something to be provided. For example, to reset a password, or to provide standard IT Services for a new User.
Priority	A category used to identify the relative importance of an incident, problem or change. Priority is based on impact and urgency, and is used to identify required times for actions to be taken.
Impact	A measure of the effect of an incident, problem or change on business processes. Impact is often based on how service levels will be affected. Impact and urgency are used to assign priority.
Urgency	A measure of how long it will be until an incident, problem or change has a significant impact on the business. For example, a high-impact incident may have low urgency if the impact will not affect the business until the end of the financial year.

Response time

The response time commences from when a call is logged by IT and a call reference number is allocated to the incident. The response times apply to the standard University working hours only: Monday to Friday, 08:00-18:00. For example, if a Low priority (response expected within 2 working days) call is received on Tuesday at 16:00, the target response time would be Thursday at 16:00.

Resolution (Fulfilment) times

Resolution time commences from when a call is logged by IT and a call reference number is allocated to the incident. The resolution time applies to standard University working hours only: Monday to Friday, 08:00-18:00.

IT will aim to resolve all incidents on a permanent basis, however sometimes it is necessary to find an interim solution (work around) in order to restore a service with a longer-term solution following. When a workaround is implemented IT staff will update the call as on hold but not 'resolve' the incident until the permanent fix is in place.

Minimum information required from users

When logging a call, all IT staff recording an incident are expected to record the following minimum level of information where TOPdesk does not automatically populate it:

- Name/user ID
- Telephone number
- Location
- University email address, or alternative email contact address
- Description of the incident (with as much detail as possible to aid with fixing the incident)
- An estimate of the impact caused by the incident and the number of users affected
- Relevant hardware or software details (e.g. IP address, MAC address) if applicable
- Depending on the type of incident, additional service related information may be required

Changing the priority of incident tickets

Any member of IT staff may alter priority assignment on tickets if information obtained after incident was logged indicate that the initial priority was wrong. This includes feedback from the User. ITIL advises that if a user asks for the priority to be changed, it should be changed without question. If the request to change priority is later found to be unwarranted, this will be dealt with via Business Relationship Management (e.g. the IT Business Partners).

If a ticket is deemed to be part of a major incident then this should be escalated, a major incident called and the IT Major Incident Plan should be used to plan the response.

Escalation

Operators are automatically warned of a potential breach of the target resolution time when 60% of the target time is elapsed. At 80%, the line manager is also notified.

Incident priority and response/resolution targets

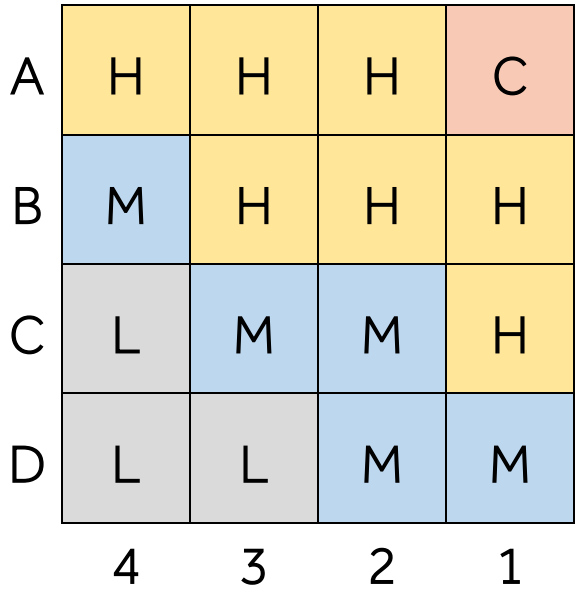
Following good practice, incident priority is made up of the product of its Urgency and Impact. Urgency relates to how important it is to resolve the incident quickly and Impact relates to the effect the incident is having on the University.

Impact

1. Whole campus, whole service, major event or major process
2. Large group of users, a group of VIPs, event or part of a service
3. Small group of users or a VIP
4. Single user

Urgency

A. Critical work impossible or life, security or reputation at risk
B. Some work impossible or moderate health, security or reputation implications
C. Reduced efficiency or minor health, security or reputation implications
D. Inconvenience



PRIORITY	TARGET RESPONSE	TARGET RESOLUTION
Critical **Possible Critical Incidents**	30 minutes	1 working day
High	1 working hour	1 working day
Medium	1 working day	3 working days
Low	2 working days	5 working days
Requests for services	As specified in SLA for service	As specified in SLA for service

Examples

- The entire email service (1) is not useable (A) = **Critical**
- An entire team (3) can't access a shared drive (B) = **High**
- The Wren service (2) is running slowly (C) = **Medium**
- A single user (4) has to type their password every time they open Outlook (D) = **Low**
- Someone (4) who relies on their phone to do their job can't make calls (A) = **High**
- A cable creating a possible trip hazard (C) is identified in a single occupancy office (4) = **Low**
- All computer users (1) have to type their password to access the internet (D) = **High**

Critical priority – and critical incidents

The term 'Major Incident' should be reserved for Major Incidents covered by the University's corporate Major Incident procedure and agreed as such by the relevant Gold Team member (e.g. typically involving risk of death, injury, reputation). In most cases IT should use the term Critical Incident when communicating with users and customers.

Description

An incident which has a priority of critical and which satisfies any of the following criteria:

- Prevents the effective use of any major service (e.g. email, Internet, Blackboard)
- Seriously affects a substantial number of users or departments
- Implies a serious breach of security
- Has a serious implication for the reputation of the University
- Has an immediate and potentially serious Health and Safety implication
- In the opinion of an IT manager or team leader is serious and requires immediate attention
- Occurs during a busy/critical period e.g. exam time, new student intake, clearing, term time

will be declared a Critical IT Incident and will invoke the Critical IT Incident Plan.

Response target

To respond to incidents within 30 minutes.

Resolution target

To resolve incidents within one day.

Escalation

All incidents with a priority Critical will immediately be escalated to IT management. If deemed appropriate, a Critical Incident will be called and a Critical Incident Manager will be designated to deal with the incident. The Critical Incident Manager will follow the IT Critical Incident Plan.

All Critical incidents will be reviewed promptly after their resolution.

Updates

The IT Major Incident Manager will keep key IT staff updated (e.g. IT Directorate and senior managers) and will co-ordinate regular updates to stakeholders (e.g. departmental managers and Heads of School), via the IT Business Partners.

The latest information about the health (or otherwise) of the service will be provided on the IT Status Page.

Examples

- Major University System failure e.g. email, Blackboard, RISIS, file servers, external web site
- Complete or significant loss of campus network connectivity
- Complete or significant loss of the telephone network
- A network problem on the readingConnect service which affects an entire hall or several halls
- A significant, malicious, security attack
- Fire/flood of a building

High Priority

Description

An incident that satisfies any of the following criteria:

- Prevents the effective use of any service and affects a substantial number of computer users, telephones or lecture/conference rooms
- Impacts an important business critical process
- Implies a breach of security
- Has possible implications for the reputation of the University
- Has very serious implications for an individual user
- Has moderate health and safety implication

Response target

To respond to incidents within one working hour.

Resolution target

To resolve incidents within one working day.

Updates

If appropriate (e.g. if the incident affects a significant number of users), the latest information will be updated on the IT Status Page.

Examples

- Server down that prevents a group of users from being able to operate as normal (i.e. inhibits their usual business processes)
- Degradation of Internet connectivity affecting a group of users (e.g. 50 people or more)
- Department file share out of file space
- Printer not working that affects many users without alternative printer available
- Partial loss of campus network access or telephone connectivity unavailable in a building
- A crucial PC that is down and is used for teaching (e.g. lecture theatre PC affecting a substantial number of attendees)
- A network problem on the readingConnect service which affects 20 or more rooms
- VIPs affected

Medium priority

Description

An incident that satisfies any of the following criteria:

- Causes inconvenience to a small number of computer or telephone users or a lecture theatre presentation
- An important service is available but performance is poor
- Affects the provision of teaching and learning for a class or meeting
- Has minor health and safety implications

Response target

To respond to incidents within 1 working day.

Resolution target

To resolve incidents within 3 working days. Updates

For incidents affecting a significant number of users, updates will be placed on the IT Status Page.

Examples

- Telephone or Network fault affecting an office with multiple occupancy
- A team unable to send or receive non-vital email via a group account
- Group printer unavailable
- Email slow for a small number of users

Low Priority

Description

An incident that satisfies any of the following criteria:

- Causes inconvenience to an individual
- A "limited support" category, for example an external SLA for non-essential equipment
- Small impact on business operations for an individual

Response target

To respond to incidents within 2 working days.

Resolution target

To resolve incidents within 5 working days.

Updates

Users will be able to contact the IT Service Desk for any updates to the incident.

Examples

- A user requires assistance with modifying a Word document in a particular way
- A user having problems with a setting that is inconvenient but does not stop them working
- Single user PC not working correctly (e.g. an application problem)
- A problem on readingConnect affecting a single user